

REMARKS/ARGUMENTS

Claims 2-12, 14-24 and 27-28 are pending with Claims 27 and 28 being the independent claims.

The Examiner has rejected Claims 10-12, 16-18, 27 and 28 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,139,723 (Conkwright, et al.) in view of U.S. Patent No. 7,055,165 (Connelly). This rejection is respectfully traversed for at least the following reasons.

Conkwright is directed to a system and method for using mathematical analysis of datasets to determine correlations and trends in television viewer behaviors. Set top box identity is involved and, as such, a mechanism for protecting privacy is required. The Examiner cites three distinct parts of Conkwright (col. 4 line 58 to col. 5, line 17; col. 10 lines 55-65; and col. 11, lines 5-39) and asserts that these disclose all the elements of Claims 27 and 28 but for the encrypting/decrypting features. However, with particular regard to the claimed feature:

Substituting said source identification indicia with anonymous identification indicia, wherein said anonymous identification indicia can be traced back to the source by a cable operator entity of the cable television system but cannot be traced back to the source by a third party...

the Examiner cites col. 4, line 58 to col. 5, line 17, as well as col. 11, lines 5-17:

Traditional set-top boxes include a unique identification number ("ID"), and this number can be used by a preferred embodiment of the present invention for identification purposes in lieu of personal information. To facilitate data analysis, a cable company can provide to the present invention *a geographically associated code, such as, but not limited to, a zip code or telephone number prefix, that corresponds with each set-top box*. Given this information, set-top box ID's to be monitored can be chosen through various means, including, but not limited to, the present invention selecting set-top box ID's at random, the present invention selecting set-top box ID's based on geographic coverage, a cable company selecting ID's based on its own criteria, or selecting all set-top box ID's. A combination of set-top box ID and geographically associated codes allows the present invention to maintain participant privacy while still allowing for determination of detailed demographic information through the inverse mathematical methods described herein.

Although privacy is an important part of the present invention, an alternative embodiment would allow set-top box operators to request a list of their viewing habits. This might be useful for parents or businesses wishing to monitor programs watched by their children or employees during a given day, or parents or businesses wishing to monitor other DATA1 datasets, such as internet viewing behaviors exhibited by employees or family members. (Emphasis added, Konkwright, col. 4, line 58 to col. 5, line 17).

and

A preferred embodiment of the present invention also provides a server with access to information from a customer billing database (Block 1104). Such billing system access can provide correlations between set-top boxes and customer data, such as billing zip code, billing area code and prefix, and the like. *To address privacy issues regarding viewership, a preferred embodiment of the present invention will identify set-top box data by zip code, area code and prefix, or other geographic identifier associated with a region in which a set-top box resides.* Correlations between set-top boxes and zip codes can be maintained in a cable television or other content provider's billing system; thus, access to such billing data may be preferred.

A highly available and highly reliable server is preferred for set-top box event monitoring, as such a devices may reside in a rack at a head-end bunker, and head-end bunkers may be physically disparate or in remote regions. A preferred embodiment of Server 1106 includes a UNIX-based server; a UNIX-based server is preferred as such servers may reduce maintenance requirements. In addition, backup circuits may be implemented to provide fault tolerance depending on availability requirements for gathered data.

Server 1106 can also attach to a network access device (Block 1107) to upload data gathered from set-top boxes to a data center. Such network access devices can include, but are not limited to, modems, routers, and satellite transceivers. As illustrated in FIG. 11, a private network link (Block 1108) is preferred for connecting a server to a data center for data uploads, as well as network and systems management, and for other functions. However, such functions may also be accomplished across a shared network, such as the Internet. Data transmitted across public or private networks may be encrypted or otherwise encoded to reduce the likelihood that such data may be used by unauthorized individuals. (Emphasis added, Konkwright, col. 11, lines 5-39).

It should be noted that in none of the above Konkwright citations is there any discussion about “anonymous identification indicia”. In fact, col. 11, lines 10+, Konkwright explains that to address privacy issues, a set top box (STB) is identified by zip code, area code and prefix or other geographic identifier associated with a region where the STB resides. Such criteria can easily be traced back by a third party. This *teaches away* from the use of anonymous identification indicia. Thus, Applicants respectfully assert that Konkwright does not teach or suggest the claimed element “substituting said source identification indicia with anonymous

identification indicia” of Claim 27 or 28.

Furthermore, Connelly is directed to a system/method for periodically deriving an optimal batch broadcast schedule based on client demand feedback data from a distributed set of broadcast clients. The Examiner asserts that Connelly provides the feature of encryption/decryption of a message and cites the following portion of Connelly:

As discussed above, automatically-generated ratings may be derived from a combination of a user's previous viewing habits (i.e., in response to pieces of content that have are currently cached or have been previously cached), and previous ratings and classification provided by the user and through use of the relevance and believability factors. In some instances, data pertaining to a user's previous viewing habits may not be used due to privacy concerns. However, in order to overcome most privacy concerns, in one embodiment the client demand feedback data is sent back to the broadcast center through a mechanism that is guaranteed not to identify from which client and/or user that set of client demand feedback data was sent. For example, this "anonymous" client scheme could be implemented through an encryption process that uses a third party as a proxy, wherein the client demand feedback data is encrypted and must pass through a decryption service operated by the third party that uses a private key that is not accessible to the broadcast operations center or any other party. *The third party then forwards the client demand feedback data to the broadcast operations center. In this manner, there is no way for the broadcast operations center to tell from which client system a given set of client demand feedback data is received.* (Emphasis added, Connelly, col. 23, lines 1-23).

In accordance with the cited portion of Connelly above, this involves concealing the identity of the end user from the broadcast operations center while having a third party act as the identity concealing agent. But this is just the opposite of what is being done in the present invention, where the cable operator knows the identity (but not the content) of the end user while the identity of the end user remains unknown to the third party (e.g., viewer behaviorship entity). See page 11, lines 11-19 of the present invention. Claims 27 and 28 were previously amended to point out this distinction, namely:

(Claim 27) ...substituting said source identification indicia with anonymous identification indicia, and wherein said anonymous identification indicia can be traced back to the source by a television service provider but cannot be traced back to the source by a third party; and

And

(Claim 28)...means for generating anonymous identification indicia and for substituting the source identifier indicia with said anonymous identification indicia to form a first decrypted message having said anonymous identification indicia embedded therein, wherein said anonymous identification indicia can be traced back to the source by a television service provider but cannot be traced back to the source by a third party;

Thus, in view of the foregoing, Applicants submit that even if one skilled in the art were to combine Conkwright with Connelly as suggested by the Examiner, the result would still not teach or suggest the invention as specified in Claims 27 and 28. Applicants, therefore, respectfully request that the §103(a) rejection be withdrawn and Claims 27 and 28 be moved to allowance.

With regard to dependent Claims 10 and 16, since these depend from Claims 27 and 28 respectively, they are patentable for the same reasons.

With regard to dependent Claims 11, 12, 17 and 18, since these depend from Claims 27 and 28 respectively, they are patentable for the same reasons.

With regard to dependent Claims 2, 3, 14 and 15 which are directed to the anonymous identification indicia using a hash algorithm, the Examiner rejects these claims under §103(a) citing U.S. Patent Publication No. 2001/0036224 (Demello, et al) as teaching the generation of anonymous identification indicia (viz., para. 0136 of Demello). Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons. Moreover, as discussed earlier, the fact that Conkwright uses zip code data, area code data or other geographic data, i.e., simple well-known location data, for forming end user identifiers this would not motivate one skilled in the art to leap to the use of pseudorandom numbers created by hash algorithms for generating identifiers. The Examiner is using the present invention as a template to assert that one skilled art would combine the

teachings of Demello with Conkwright and Connelly to arrive at the inventions of Claims 2, 3, 14 and 15. Thus, Applicants respectfully request the withdrawal of the §103(a) rejection regarding Claims 2, 3, 14 and 15.

With regard to dependent Claims 4, 5, 19 and 20 regarding secure locations wherein access to a computer is controlled, the Examiner rejects these claims under §103(a) citing U.S. Patent No. 6,598,231 (Basawapatna, et al.) as teaching the use of a secure facility. This patent suggests the use of providing secure buildings and structures for all headend, node and service module equipment. Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons.

With regard to dependent Claims 6 and 21, which are directed to the cable operator entity not having access to the password of a computer in a structure that only the cable operator entity has access to, the Examiner rejects these claims under §103(a) citing the Handbook of Applied Cryptography by Menezes, et al., as demonstrating that a certain user has a password to gain access to a computer. Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons.

With regard to dependent Claims 7, 8, 22 and 23 which specify the insertion of cable system source data into the first decrypted message, the Examiner rejects these claims under §103(a) citing U.S. Patent No. 5,390,173 (Spinney, et al.) as teaching the insertion of network segment data into packets, but there is no discussion about cable system network segment data. Thus, Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons.

With regard to dependent Claims 9 and 24 which specify including cluster code data into

Application Serial No. 10/628,173
Attorney Docket No. Q1014/20014
Request for Reconsideration Dated June 20, 2008

the encrypted message, the Examiner rejects these claims under §103(a) citing U.S. Patent Publication No. 2002/0059632 (Link, et al.), as already disclosing this feature. Applicants respectfully submit that because these claims ultimately depend from Claims 27 and 28 respectfully, they are also patentable for the same reasons.

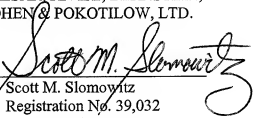
Thus, Applicants respectfully submit that Claims 2-12, 14-24 and 27-28 are in condition for allowance. Accordingly, prompt and favorable examination on the merits is respectfully requested.

Should the Examiner believe that anything further is desirable in order to place the application in even better condition for initial examination and allowance, the Examiner is invited to contact Applicant's undersigned attorney at the telephone number listed below.

Respectfully submitted,

CAESAR, RIVISE, BERNSTEIN,
COHEN & POKOTILOW, LTD.

By


Scott M. Slomovitz
Registration No. 39,032
Customer No. 03000
(215) 567-2010
Attorneys for Applicants

June 20, 2008

Please charge or credit our
Account No. 03-0075 as necessary
to effect entry and/or ensure
consideration of this submission.